Engineer

Зворотний проксі

← сервер, що приймає запити від імені вебслужби

Що це таке

Зворотний проксі приймає запити від імені вебслужби. Браузер з'єднується з публічною адресою сайту. Проксі приймає запит на цій адресі, передає його потрібному серверу й повертає браузеру відповідь. Сервер за проксі називають вихідним сервером. Він може змінити порт, адресу чи навіть мережу, а відвідувачі й далі користуватимуться тими самими посиланнями. Стандарт HTTP називає цю роль шлюзом. Прямий проксі діє з боку клієнта й звертається до інших вузлів від його імені.

Уявімо сайт, який завантажує головну сторінку з однієї служби, а звіт за шляхом `/api/reports/42` з іншої. Для браузера обидва ресурси належать одному домену. Проксі читає шлях HTTP-запиту й обирає потрібну службу. Якщо один звіт можуть підготувати кілька рівноцінних серверів, проксі також може розподіляти між ними навантаження. Маршрутизація за шляхом і розподіл навантаження є окремими завданнями. Проксі з одним сервером за ним теж дає змогу відокремити публічну адресу від внутрішньої.

Деякі системи вміють просто передати зашифроване з'єднання TCP до потрібного вузла. У цьому режимі вони можуть скористатися відомостями про з'єднання та видимими полями початкового обміну TLS, якщо такі поля доступні. Маршрутизація за зашифрованим шляхом потребує доступу до повідомлення HTTP. На схемі мережі варто показати, де закінчується TLS-сеанс браузера і чи відкриває проксі окреме зашифроване з'єднання до вихідного сервера.

Застосуйте поняття до рішення

Застосуйте «Що таке зворотний проксі?» до конкретного рішення. Ми можемо пов'язати поняття із системою, яку ви створюєте або купуєте. Wi-Fi, фаєрволи і віддалений доступ налаштовані так, щоб працювати можна було звідусіль, а заходити — лише своїм.

Переглянути наші послуги Зв'язатися з нами →

Перевірте припущення за терміном

Використайте пояснення та пов'язані роботи, щоб сформулювати запитання для проєкту. Ми можемо перевірити припущення разом до вибору інструмента. Керувала 30 інстансами Ubuntu Linux VPS — 30 серверів Linux під управлінням, із планом відновлення

Керувала 30 інстансами Ubuntu Linux VPS Зв'язатися з нами →

Чому це важливо

Спільна точка входу визначає, до яких служб можна звертатися ззовні. Проксі може керувати сертифікатом публічного домену, тимчасом як застосунки доступні лише в приватній мережі. На вході можна вести журнал доступу, перевіряти розмір запитів і застосовувати правила переспрямування. Умови залежать від маршруту. Службі завантаження файлів потрібен більший допустимий розмір запиту, а службі потокової передачі може бути важливо надсилати клієнтові частини відповіді відразу.

На проксі, що завершує TLS, відкривається вміст запиту. Оператор такого вузла може бачити файли cookie, параметри пошуку й дані, які ввів користувач. Наступне зашифроване з’єднання захищає трафік до вихідного сервера під час передавання. Межа довіри охоплює точку, де дані розшифровуються. Варто заздалегідь визначити, хто керує проксі, які поля потрапляють до журналу та кому дозволено його читати.

Додатковий вузол змінює пошук причин відмови. Шлюз може видати `502`, якщо отримав некоректну відповідь, або `504`, якщо не дочекався відповіді в установлений час. Застосунок теж може повернути код помилки. Зіставте записи про один контрольний запит, його час і статус на обох вузлах. Якщо запит не надійшов до вихідного сервера, перевірте стан з’єднання між цим сервером і проксі.

Як це виглядає на практиці

У прикладі звірення DNS-зони, описаної кодом Engineer ApS розповідає про налаштований CDN-проксі, який працював і згодом був вимкнений. Коли трафік ішов через мережу постачальника, він міг обробляти IP-адреси відвідувачів і запитані ними URL ще до того, як запит доходив до компанії. У цьому випадку компанія надала перевагу приватності перед додатковим захистом від атак. DNS-зона залишилася придатною для зберігання у системі керування версіями й перевірки. Приклад допомагає окремо оцінити того, хто обслуговує DNS, і того, хто приймає вебзапити.

У тестовому середовищі надішліть запити до `/health` та `/api/reports/42?view=summary` . Перевірте, який метод і шлях отримує застосунок. У браузері перевірте статус, публічну адресу та схему кожного переспрямування. Змініть внутрішню адресу служби звітів і повторіть запити з тим самим публічним іменем. Так можна перевірити, що посилання залишаються придатними після перенесення служби.

Перед увімкненням спільного кешу відкрийте два сеанси з різними тестовими обліковими записами. Додайте до відповіді кожного сеансу свій безпечний маркер і перевірте, що вміст не переходить між ними. Наприкінці навмисно зупиніть вихідний сервер у тестовому середовищі й виміряйте, коли браузер отримає помилку. Збережіть відповідний запис журналу, щоб під час збою знати, як виглядає відмова на цій ділянці.

Де виникають проблеми

Клієнт з інтернету може сам додати заголовок `Forwarded` або `X-Forwarded-For` . Застосунок має знати перелік посередників, від яких він приймає такі відомості. Вилучайте або замінюйте неперевірені значення на вході й обмежте прямі з’єднання до вихідного сервера. Надішліть контрольний запит з вигаданою адресою. Перевірте, яку адресу застосунок записав і яку використав для ухвалення рішення про доступ.

Про неправильну публічну адресу іноді свідчить цикл переспрямувань. Браузер під’єднався через HTTPS, а застосунок сформував посилання для повернення через HTTP або додав внутрішній порт. Передайте застосунку перевірені публічну схему та ім’я вузла. Пройдіть увесь процес входу, зокрема повернення з іншого сервісу, і перевірте файли cookie. Якщо проксі відтинає початок шляху, задайте вкладений шлях із параметрами, щоб точно побачити результат.

Повторення після перевищення часу очікування може виконати дію двічі. Наприклад, застосунок міг уже зафіксувати оплату, коли проксі припинив чекати на відповідь. Визначте, як застосунок розпізнає повтори, перш ніж дозволяти автоматичне повторення запитів, що змінюють дані. Після контрольної дії затримайте відповідь у тестовому середовищі. Перевірте, яке з’єднання закривається першим і чи можна за журналами відновити порядок подій.

Що почитати далі

- RFC 9110 про посередників HTTP визначає роль проксі, шлюзу й тунелю.
- RFC 7239 про Forwarded пояснює, як передавати відомості та враховувати безпеку й приватність.
- Модуль HTTP-проксі NGINX описує маршрути, заголовки, буферизацію та час очікування.
- Директива reverse_proxy у Caddy пояснює вибір сервера й опрацювання заголовків.
- Посібник Apache HTTP Server показує, як публічний сервер передає запити внутрішнім службам.

Словник

Обирайте за фактичними умовами

Опишіть шлях розгортання, експлуатаційні ризики та чергову команду. Ми можемо визначити зміну з перевірками, шляхом відновлення та чіткою відповідальністю.

Дивитися, скільки це коштує Зв'язатися з нами →

Зробіть термінологію практичною

Запитайте, як «Що таке зворотний проксі?» стосується вашої організації. Конкретного прикладу з поточної системи достатньо для початку розмови.

Переглянути наші послуги

welcome@engineer.company +45 50 10 61 84 Копенгаген, Данія

Візьміть цю сторінку із собою

Візитівка

Дбайливо зроблено з любов'ю — D.

CVR 45969703 · Tagensvej 105C, 3. th, 2200 København N

Авторське право © 2025 – дотепер · Engineer ApS · Усі права захищено.

Надруковано з https://engineer.company/uk/glossary/reverse-proxy/